(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－251323
（P2002－251323A）
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G06F	12/14	310	G06F 12/14	310K	5B017
	12/00	537	12/00	537A	5B082
		545		545A	5B085
	15/00	330	15/00	330D	

審査請求　未請求　請求項の数３　ＯＬ　（全 17 頁）

(21)出願番号　特願2001－45151(P2001－45151)

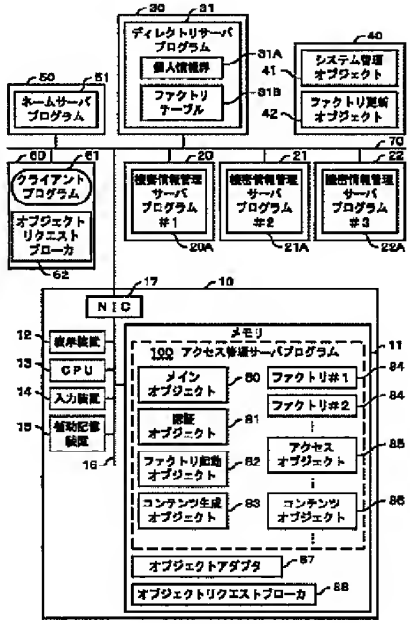
(22)出願日　平成13年２月21日(2001.2.21)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　寺崎　仁
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100083378
弁理士　松村　勝

Ｆターム(参考)　5B017 AA03 BA06
5B082 EA11 HA00
5B085 AE06 BG07

(54)【発明の名称】　アクセス管理プログラム

(57)【要約】
【課題】　アクセスポリシー又はシステム構成の変更にアクセス管理プログラムを比較的簡単に適合させる。
【解決手段】　複数のアクセスレベルに対応する複数のファクトリ８４をディレクトリサーバプログラム３１内のファクトリテーブル３１Ｂ内に記憶させる。ユーザのアクセスレベルに対応するファクトリをメモリ１１にロードし、そのファクトリによりユーザがアクセス権限を有する複数の機密情報管理サーバプログラムをそれぞれアクセスするための複数のアクセスメソッドを含むアクセスオブジェクト８５を当該ユーザに対応して生成する。ユーザがいずれかの機密情報をアクセス先に選択したとき、アクセスオブジェクト８５に含まれたアクセスメソッドにより、当該機密情報を管理するサーバプログラム２０Ａにアクセスする。



1

【特許請求の範囲】

【請求項１】　ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するための前記一群の機密情報に共通に設けられたアクセス管理プログラムであって、

前記一群の機密情報のうち、前記アクセス管理プログラムにアクセスしてきたユーザに割り当てられたアクセスレベルに対応してあらかじめ定められた少なくとも一つの機密情報に前記ネットワークを介してアクセスするための少なくとも一つのアクセスメソッドを含むアクセスオブジェクトを当該ユーザに対応して生成し、

前記少なくとも一つの機密情報に対する前記ユーザからのアクセス要求を受け付け、前記少なくとも一つのアクセスメソッドを用いて当該少なくとも一つの機密情報にアクセスする、

ステップをコンピュータに実行させることを特徴とするアクセス管理プログラム。

【請求項２】　前記生成するステップは、複数のアクセスレベルに対応してあらかじめ生成された、オブジェクトを生成するための複数のファクトリのうち、前記ユーザに割り当てられたアクセスレベルに対応する一つのファクトリにより、前記アクセスオブジェクトを生成する、

ことを特徴とする請求項１に記載のアクセス管理プログラム。

【請求項３】　前記複数のファクトリは、前記アクセス管理プログラムを実行時に記憶するためのメモリと異なる記憶手段にあらかじめ記憶され、

前記生成するステップは、

前記一つのファクトリが前記記憶手段から前記メモリに既にロードされているか否かを判別し、

当該ファクトリがまだロードされていないと判断されたとき、前記記憶手段から前記メモリに当該ファクトリをロードし、

前記ロードされたファクトリにより前記アクセスオブジェクトを生成する、

ステップを含むことを特徴とする請求項２記載のアクセス管理プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するためのアクセス管理プログラム、アクセス管理システム、アクセス管理方法に関する。

【０００２】

【従来の技術】従来、ネットワークに接続された複数のコンピュータノードに実装された一群の機密情報管理サーバプログラムが複数の機密情報サービスを提供し、ユーザがこれらの機密情報サービスをネットワークを介して利用できるようになっている。ユーザにあらかじめアクセスレベルを割り当て、アクセスレベルに応じてユーザが利用できる機密情報サービスを制限する方法が一般に取られている。アクセスレベルと当該アクセスレベルのユーザがアクセス権限を有する機密情報サービスとの関係は、コンピュータシステムのシステム管理者によりあらかじめ定められ、アクセスポリシーとも呼ばれる。

【０００３】ユーザによる機密情報サービスの利用の可否を制御するためにアクセス管理サーバプログラムが上記複数の機密情報管理サーバプログラムに共通に設けられ、ユーザはいずれかの機密情報サービスを使用するときには、まず当該アクセス管理サーバプログラムにアクセスする。当該アクセス管理サーバプログラムが、ユーザが選んだ機密情報サービスを利用する権限を有するか否かを当該ユーザのアクセスレベルに基づいて判断し、ユーザが当該機密情報サービスを利用する権限を有するときには、当該機密情報サービスを提供する機密情報管理サーバプログラムへアクセスしていた。

【０００４】

【発明が解決しようとする課題】しかしながら、従来技術では、アクセスポリシーの変更あるいは利用可能な一群の機密情報管理サーバプログラムに関する変更、追加、削除（以下、システム構成の変更とも呼ぶ）が生じたとき、機密情報管理サーバプログラムをその変更に適合させるために多くのプログラム変更作業を要していた。

【０００５】したがって、本発明の目的は、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時に、その変更に比較的簡単に適合させるのに適したアクセス管理プログラムを提供することである。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明に係るアクセス管理プログラムは、ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するための前記一群の機密情報に共通に設けられたアクセス管理プログラムであって、前記一群の機密情報のうち、前記アクセス管理プログラムにアクセスしてきたユーザに割り当てられたアクセスレベルに対応してあらかじめ定められた少なくとも一つの機密情報に前記ネットワークを介してアクセスするための少なくとも一つのアクセスメソッドを含むアクセスオブジェクトを当該ユーザに対応して生成し、前記少なくとも一つの機密情報に対する前記ユーザからのアクセス要求を受け付け、前記少なくとも一つのアクセスメソッドを用いて当該少なくとも一つの機密情報にアクセスする、ステップをコンピュータに実行させるもので

ある。

【０００７】このようにアクセスレベルに対応して定められたアクセスオブジェクトをユーザに対応して生成して使用することにより、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成が変更されたとき、ユーザ対応に生成する上記アクセスオブジェクトに含まれるメソッドを変更するように、アクセス管プログラムを変更するという比較的簡単な作業により、アクセスポリシー又はシステム構成の変更にアクセス管理プログラムを適合させることができる。

【０００８】具体的には、前記生成するステップは、複数のアクセスレベルに対応してあらかじめ生成された、オブジェクトを生成するための複数のファクトリのうち、前記ユーザに割り当てられたアクセスレベルに対応する一つのファクトリにより、前記アクセスオブジェクトを生成する。

【０００９】このようにアクセスレベルに対応して定められたアクセスオブジェクトを生成するためのファクトリを用いることにより、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時にファクトリを更新するという比較的簡単な作業によりアクセス管理プログラムをアクセスポリシー又はシステム構成の変更に適合させることができる。

【００１０】更に具体的には、前記複数のファクトリは、前記アクセス管理プログラムを実行時に記憶するためのメモリと異なる記憶手段にあらかじめ記憶され、前記生成するステップは、前記一つのファクトリが前記記憶手段から前記メモリに既にロードされているか否かを判別し、当該ファクトリがまだロードされていないと判断されたとき、前記記憶手段から前記メモリに当該ファクトリをロードし、前記ロードされたファクトリにより前記アクセスオブジェクトを生成する、ステップを含む。

【００１１】これにより、アクセスポリシー又はシステム構成の変更時に前記記憶手段に記憶されたファクトリを変更するというより簡単な方法により、アクセスポリシー又はシステム構成の変更にアクセス管理プログラムを適合させることができる。

【００１２】

【発明の実施の形態】以下、本発明に係るアクセス管理プログラムの実施の形態を図面を参照して詳細に説明する。

【００１３】図１は、本発明に係るアクセス管理プログラムの一つの実施の形態を用いたコンピュータシステムのブロック図である。図において、１０、２０、２１、２２、３０、４０、５０、６０は、コンピュータノードであり、例えばＬＡＮ７０のようなネットワークに接続されている。本コンピュータシステムは例えば企業等の団体の内部で使用されるシステムである。

【００１４】コンピュータノード１０は、例えばワークステーションにより構成される。より具体的には、コンピュータノード１０は、メモリ１１、表示装置１２、中央処理装置（ＣＰＵ）１３、キーボード及びマウス等のポインティングデバイスを備える入力装置１４、補助記憶装置１５、これらを接続するバス１６と、バス１６とＬＡＮ７０とを接続するネットワークインターフェースカード１７よりなる。他のノードコンピュータも同様であるが、図には他のノードコンピュータに関しては当該ノードコンピュータのメモリに記憶されたプログラムあるいはデータのみを簡単化のために示している。

【００１５】コンピュータノード１０は、アクセス管理サーバプログラム１００を実行する。コンピュータノード２０、２１、２２は、機密情報サービスを提供する機密情報管理サーバプログラム２０Ａ、２１Ａ、２２Ａをそれぞれ実行する。これらのプログラムは、機密情報を含むデータベースをコンピュータノードに内蔵された図示しない補助記憶装置に記憶して管理する。機密情報管理サーバプログラムが実行されるコンピュータノードの数は一つ又は複数であればよく、その数は特に制限されないが、図には一例として３つのコンピュータノード２０、２１、２２が示されている。

【００１６】コンピュータノード３０は、ディレクトリサーバプログラム３１を実行する。ディレクトリサーバプログラム３１は、複数のユーザに関する個人情報群３１Ａと後に述べるオブジェクトを生成するためのオブジェクトである複数のファクトリを内部に含むファクトリテーブル３１Ｂ等を、内蔵する補助記憶装置（図示せず）に階層構造を用いて記憶し管理する。コンピュータノード４０は、システム管理オブジェクト４１及びファクトリ更新オブジェクト４２を実行する。これらのオブジェクトは、アクセスポリシー又はシステム構成の変更時にコンピュータシステムのシステム管理者によりアクセス管理サーバプログラム１００の更新のために使用される。

【００１７】コンピュータノード５０は、本コンピュータシステムのためのネームサーバプログラム５１を実行する。コンピュータノード６０は、機密情報管理サーバプログラム２０Ａ、２１Ａ、２２Ａ等を利用するユーザにより使用されるクライアントプログラム６１を実行する。クライアントプログラム６１を実装したコンピュータノードは実際には複数個存在するが、図には簡単化のための一つのコンピュータノード６０のみを示す。本コンピュータシステムは、各コンピュータノード内の各プログラムがオブジェクトにより構成されている分散オブジェクトシステムを実現している。

【００１８】本コンピュータシステムでは、ユーザにはあらかじめ複数のアクセスレベルの一つが割り当てられ、各アクセスレベルに対応して、アクセスが許される一つ又は複数の機密情報が定められている。具体的には、各アクセスレベルに対応して、機密情報管理サーバ

プログラム２０Ａ、２１Ａ、２２Ａのうちアクセスが許される一つ又は複数の機密情報管理サーバプログラムがあらかじめ定められている。すなわち、機密情報管理サーバプログラム２０Ａ、２１Ａ、２２Ａに対する各ユーザのアクセス権限は、当該ユーザに割り当てられたアクセスレベルに依存して定められている。アクセスレベルと当該アクセスレベルのユーザがアクセスを許される機密情報管理サーバプログラムとの関係（アクセスポリシー）は、コンピュータシステムのシステム管理者によりあらかじめ定められる。

【００１９】本発明に係るアクセス管理プログラムの一つの実施の形態は、アクセス管理サーバプログラム１００、個人情報群３１Ａ、ファクトリテーブル３１Ｂ、システム管理オブジェクト４１、ファクトリ更新オブジェクト４２により実現されている。本発明に係るアクセス管理システムの一つの実施の形態は、コンピュータノード１０、３０、４０とそれらに実装されたプログラムにより実現される。各ユーザは、機密情報管理サーバプログラム２０Ａ、２１Ａ、２２Ａのいずれかにより提供される機密情報サービスを利用したいとき、クライアントプログラム６１を介してアクセス管理サーバプログラム１００にアクセスする。

【００２０】アクセス管理サーバプログラム１００は、ユーザの認証を行い、ユーザの正当性を確認した後に、当該ユーザにアクセス権限が与えられた一つ又は複数の機密情報管理サーバプログラムにより管理されている機密情報に対するユーザのアクセス要求を受け付け、当該機密情報管理サーバプログラムと当該ユーザが使用するクライアントプログラム６１との間の通信を中継する。当該ユーザにアクセス権限が与えられていない他の機密情報管理サーバプログラムにより管理されている機密情報に対するアクセス要求は受け付けられない。

【００２１】より具体的には、当該ユーザがアクセス権限を有しない一つ又は複数の機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有し、当該ユーザがアクセス権限を有しない機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有しないアクセスオブジェクトを当該ユーザに対応して生成し、このアクセスオブジェクトを用いてユーザがアクセス権限を有する機密情報管理サーバプログラムへのアクセスを実行し、当該機密情報管理サーバプログラムとユーザが使用するクライアントプログラムとの間の通信を中継する。

【００２２】コンピュータシステムの運用の過程で、アクセスポリシーが変更されることがある。すなわち、あるアクセスレベルについて、当該アクセスレベルを有するユーザがアクセス権限を与えられていた機密情報管理サーバプログラムに対してアクセス権限が与えられなくなったり、あるいはその逆のことが起きる。あるいはアクセスレベルが追加されたり削減されたりすることが生じる。

【００２３】さらにはシステム構成が変更されることがある。すなわち、本コンピュータシステムで利用可能な機密情報管理サーバプログラムが変更、追加又は削除されたり、あるいはそれらが実装されるコンピュータノードが変更になることがある。

【００２４】アクセスポリシーの変更又はシステム構成の変更が発生したとき、コンピュータノード４０に対するシステム管理者の指示入力にしたがって、各ユーザに対応して生成する上記アクセスオブジェクトとして、変更後のアクセスポリシー又は変更後のシステム構成に対応したアクセスオブジェクトが生成される。

【００２５】アクセス管理サーバプログラム１００は、図示するように、コンピュータノード１０のメモリ１１に実装されたメインオブジェクト８０、認証オブジェクト８１、ファクトリ起動オブジェクト８２、コンテンツ生成オブジェクト８３、複数のファクトリ８４、アクセスオブジェクト８５、コンテンツオブジェクト８６等により構成される。複数のファクトリ８４は、それぞれ一つのアクセスレベルに対応して定められている。アクセスオブジェクト８５とコンテンツオブジェクト８６は、アクセス管理サーバプログラム１００にアクセスしたユーザに対応して生成される。

【００２６】分散オブジェクトシステムを実現するためのオブジェクトアダプタ８７、オブジェクトリクエストブローカ８８等のオブジェクトもメモリ１１に実装される。これらのオブジェクトは共通オブジェクトリクエストブローカアーキテクチャ（ＣＯＲＢＡ）により定義されているオブジェクトである。オブジェクトアダプタ８７は、後述するオブジェクトレファレンスを決定する機能を有し、オブジェクトリクエストブローカ８８は、異なるオブジェクト間の通信路を提供する。コンピュータノード１０を制御するＯＳもメモリ１１に実装されるが、本ＯＳは簡単化のために図示されていない。

【００２７】なお、他のコンピュータノード２０、２１、２２、３０、４０、５０、６０にもオブジェクトアダプタ、オブジェクトリクエストブローカが実装されるが、これらのオブジェクトは簡単化のために図示されていない。他のコンピュータノードに実装されるＯＳについても同様である。

【００２８】図２は、アクセス管理サーバプログラム１００により実行される一例としての処理の流れの概要を模式的に示す。アクセス管理サーバプログラム１００は、メインオブジェクト８０を起動することにより起動される。メインオブジェクト８０は、起動されると、認証オブジェクト８１、ファクトリ起動オブジェクト８２、コンテンツ生成オブジェクト８３を生成する。ユーザは、クライアントプログラム６１を介して認証オブジェクト８１にアクセスする（ステップＳ１）。

【００２９】認証オブジェクト８１は、ユーザの個人認

証を行うオブジェクトであり、ユーザが入力した識別情報に基づいてディレクトリサーバプログラム３１により管理される当該ユーザの個人情報を読み出す（ステップＳ２）。ディレクトリサーバプログラム３１は、個人情報群３１Ａとして、例えば複数のユーザの各々の電子証明書とそれに関連する情報及び他の個人情報を記憶する。ディレクトリサーバプログラム３１は、例えばディレクトリ標準ＩＴＵ Ｘ．５００にしたがって情報を記憶する。

【００３０】ユーザはユーザ認証情報として上記ディレクトリ標準で定められた当該ユーザの識別名（Distinguished Name －ＤＮ）を入力する。識別名（ＤＮ）は、例えばユーザの所属部署、氏名、電子メールアドレス等を含む。読み出された個人情報には、電子証明書に関連する情報その他の個人情報の他に、ユーザに割り当てられたアクセスレベルと、ユーザにあらかじめ割り当てられた他のユーザ識別情報（例えばユーザＩＤとパスワードの組）が含まれている。当該他の識別情報は、後に機密情報管理サーバプログラムが行う個人認証に使用される。

【００３１】認証オブジェクト８１は、ユーザが入力したユーザの識別名（ＤＮ）と読み出された個人情報とを用いて当該ユーザの正当性を確認し、ユーザの正当性が確認されると、認証オブジェクト８１は、ファクトリ起動オブジェクト８２を呼び出す（ステップＳ３）。このとき、ユーザに割り当てられたアクセスレベルと前述の他のユーザ識別情報とが引き渡される。

【００３２】ファクトリ起動オブジェクト８２は、引き渡されたアクセスレベルに対応するファクトリ８４を呼び出す。すべてのアクセスレベルに対応する複数のファクトリ８４は、ディレクトリサーバプログラム３１が管理するファクトリテーブル３１Ｂ内にあらかじめ格納されていて、各ファクトリ８４は、メモリ１１にロードされてから起動される。ファクトリ起動オブジェクト８２は、内部にロード済みファクトリテーブル８２０を有する。ロード済みファクトリテーブル８２０は、各アクセスレベルに対応するファクトリ８４がメモリ１１に既にロードされているか否かを示すデータを保持している。

【００３３】ファクトリ起動オブジェクト８２は、起動されたときに、ユーザのアクセスレベルに対応するファクトリ８４がメモリ１１にロードされているか否かをこのロード済みファクトリテーブル３２０を参照して判断し、そのファクトリがまだメモリ１１にロードされていないときには、ファクトリテーブル３１Ｂからメモリ１１にそのファクトリ８４をロードし（ステップＳ４）、起動する（ステップＳ５）。そのファクトリ８４が既にメモリ１１にロードされているときには、ファクトリ起動オブジェクト８２は、そのロード済みのファクトリ８４を起動する（ステップＳ５）。起動時に前述の他のユーザ識別情報が引き渡される。

【００３４】起動されたファクトリ８４は、対応するアクセスレベルを有するユーザがアクセス権限を有する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有するアクセスオブジェクト８５を生成する（ステップＳ６）。このとき、ファクトリ８４から前述の他のユーザ識別情報がアクセスオブジェクト８５に引き渡される。こうして特定のユーザに対応してアクセスオブジェクト８５が生成される。

【００３５】このアクセスオブジェクト８５の参照値は、ファクトリ８４からファクトリ起動オブジェクト８２に戻され（ステップＳ７）、更にファクトリ起動オブジェクト８２から認証オブジェクト８１に戻される（ステップＳ８）。ここで、オブジェクトの参照値は、当該オブジェクトが存在するコンピュータノード上に存在する他のオブジェクトが当該オブジェクトを特定するために使用されるオブジェクト識別情報である。認証オブジェクト８１は、コンテンツ生成オブジェクト８３にこの参照値を指定して、コンテンツオブジェクトの生成を要求し（ステップＳ９）、コンテンツ生成オブジェクト８３は、ユーザに対応してコンテンツオブジェクト８６を生成する（ステップＳ１０）。

【００３６】コンテンツオブジェクト８６は、本コンピュータシステムで提供される複数の機密情報サービスのメニューをクライアントプログラム６１に通知する機能と、いずれかの機密情報サービスがユーザにより選ばれたときに、その機密情報サービスを実行する機密情報管理サーバプログラムへの接続要求を当該ユーザのためのアクセスオブジェクト８５に通知する機能を有する。

【００３７】コンテンツ生成オブジェクト８３は、コンテンツオブジェクト８６が生成されると、認証オブジェクト８１にコンテンツオブジェクト８６の参照値を戻す（ステップＳ１１）。認証オブジェクト８１は、コンテンツオブジェクト８６のオブジェクトレファレンスをクライアントプログラム６１に通知する（ステップＳ１２）。ここでオブジェクトのオブジェクトレファレンスは、当該オブジェクトが存在するコンピュータノードと異なるコンピュータノード上に存在する他のオブジェクトが当該オブジェクトを特定するために使用されるオブジェクト識別情報である。

【００３８】クライアントプログラム６１は、通知されたオブジェクトレファレンスを用いてコンテンツオブジェクト８６を呼び出し、メニュー表示を要求する（ステップＳ１３）。コンテンツオブジェクト８６は、クライアントプログラム６１に機密情報サービスのメニューリストデータを送る（ステップＳ１４）。クライアントプログラム６１は、このメニューリストデータに基づいて機密情報サービスの一覧を示すメニューを表示装置の画面に表示する。

【００３９】ユーザが画面上の操作によりいずれかの機密情報サービスを選択すると、クライアントプログラム

６１は、選択された機密情報サービスへの接続をコンテンツオブジェクト８６に要求する（ステップＳ１５）。コンテンツオブジェクト８６は、この要求を当該ユーザに対応するアクセスオブジェクト８５に通知する（ステップＳ１６）。

【００４０】アクセスオブジェクト８５は、ユーザがアクセス権限を有する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを内蔵している。ユーザが要求した機密情報サービスを提供する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドがアクセスオブジェクト８５に含まれている場合には、アクセスオブジェクト８５はそのアクセス要求を受け付け、そのアクセスメソッドを実行し、当該機密情報管理サーバプログラムに接続する（ステップＳ１７）。

【００４１】ユーザがアクセス権限を有しない機密情報管理サーバプログラムにアクセスするためのアクセスメソッドは、アクセスオブジェクト８５には内蔵されていない。したがって、ユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムに対してユーザがアクセス権限を有しない場合、アクセスオブジェクト８５は、当該機密情報サービスに対するユーザの機密情報利用要求を受け付けない。

【００４２】ステップＳ１７により機密情報管理サーバプログラムがアクセスされた場合、当該機密情報管理サーバプログラムがユーザの識別情報の入力を要求したときには、アクセスオブジェクト８５内の上記アクセスメソッドは、ファクトリ８４から引き継いだ前述の他のユーザ識別情報を当該機密情報管理サーバプログラムに転送する。ユーザの正当性が当該機密情報管理サーバプログラムにより認証されると、クライアントプログラム６１とユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムとの間でアクセスオブジェクト８５、コンテンツオブジェクト８６を介した通信路が開かれることになる。

【００４３】当該機密情報管理サーバプログラムは、応答情報をアクセスオブジェクト８５に戻し（ステップＳ１８）、アクセスオブジェクト８５は、その応答情報をコンテンツオブジェクト８６に戻し（ステップＳ１９）、コンテンツオブジェクト８６は、その情報をクライアントプログラム６１に戻す（ステップＳ２０）。クライアントプログラム６１に対してその後ユーザが当該機密情報管理サーバプログラムに転送すべき情報を入力した場合には、当該情報は、同様にして当該機密情報管理サーバプログラムに転送される。

【００４４】このようにしてクライアントプログラム６１とユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムとの間でアクセスオブジェクト８５、コンテンツオブジェクト８６を介したデータ通信が実行されることになる。

【００４５】他のユーザに関しても同様に対応するアクセスオブジェクトとコンテンツオブジェクトが生成され、当該他のユーザが使用するクライアントプログラムと当該他のユーザが選択した機密情報を管理する機密情報管理サーバプログラムとの間でデータ通信が、上記データ通信と独立にかつ並行して実行されることになる。

【００４６】なお、アクセスポリシーあるいはシステム構成の変更が生じたとき、アクセス管理サーバプログラム１００がコンピュータノード４０を用いてシステム管理者により更新される。具体的には、システム管理オブジェクト４１、ファクトリ更新オブジェクト４２を用いて、アクセスポリシーあるいはシステム構成の変更に伴い、変更されるべき又は不要になったファクトリがディレクトリサーバプログラム３１内のファクトリテーブル３１Ｂ及びメモリ１１から削除され、変更後のファクトリあるいは新たに必要になったファクトリがファクトリテーブル３１Ｂに追加される。

【００４７】したがって、その後はあるアクセスレベルに対応するファクトリがメモリ１１に存在しないときに、当該ファクトリはファクトリテーブル３１Ｂからメモリ１１にロードされることになり、ファクトリの変更、削除、追加等の更新が円滑に実現される。その結果、アクセスポリシー又はシステム構成の変更に適合したアクセスオブジェクトを生成することが比較的容易になる。

【００４８】以下では、アクセス管理サーバプログラム１００と関連する他のプログラムの処理の詳細を説明する。図３から図６は、組み合わせてアクセス管理サーバプログラム１００により実行される一例としての処理の概略フローチャートを示す。

【００４９】まず、クライアントプログラム６１は、アクセス管理サーバプログラム１００へのアクセスをユーザから指示されると、認証オブジェクト８１を呼び出す（ステップＳ１０１）。クライアントプログラム６１は、この呼び出しに当たり分散オブジェクトシステムで通常行われる方法により認証オブジェクト８１のオブジェクトレファレンスを取得し、上記呼び出しは取得されたオブジェクトレファレンスを用いて行われる。

【００５０】例えば、クライアントプログラム６１は、そのプログラムが実装されているコンピュータノード６０内のオブジェクトリクエストブローカ６２（図１）に、コンピュータノード５０に実装されたネームサーバプログラム５１へのアクセスを要求する。オブジェクトリクエストブローカ６２は、この要求に応答して通信オブジェクトを生成し、クライアントプログラム６１にその通信オブジェクトの参照値を戻す。

【００５１】クライアントプログラム６１は、生成された通信オブジェクトに認証オブジェクト８１のオブジェクトレファレンスを要求する。生成された通信オブジェクトは、ネームサーバプログラム５１に認証オブジェクト８１のオブジェクトレファレンスを要求する。ネーム

サーバプログラム５１は、認証オブジェクトに対応してあらかじめ記憶してあったオブジェクトレファレンスを上記通信オブジェクトに戻し、当該通信オブジェクトはそのオブジェクトレファレンスをクライアントプログラム６１に戻す。こうして、クライアントプログラム６１は呼び出すべき認証オブジェクト８１のオブジェクトレファレンスを取得することができる。

【００５２】認証オブジェクト８１は、クライアントプログラム６１により呼び出されると、内部のメソッドを実行してクライアントプログラム６１にユーザ識別情報を要求する（ステップＳ１０２）。認証は、ディレクトリサーバプログラム３１により管理される複数のユーザに対してあらかじめ記憶された個人情報群を用いて行われる。各ユーザの個人情報には、例えば図３内に示すように、当該ユーザが使用する電子証明書の認証に使用される個人情報３１０を用いることができる。

【００５３】電子証明書には例えばＩＳＯ／ＩＥＣ／ＩＴＵが定めたＸ．５０９電子証明書を使用することができる。すなわち、各ユーザの個人情報３１０は、電子証明書そのものとそれに関連する識別名（ＤＮ）その他の複数の情報及び他の個人情報を含む。電子証明書の証明に用いられる識別名（ＤＮ）は、その証明書を使用するユーザを特定するユーザ識別情報である。識別名（ＤＮ）は、例えばユーザの所属部署、氏名、電子メールアドレス等を含む。個人情報３１０に含まれる当該他の個人情報には、ユーザに割り当てられたアクセスレベル及び当該ユーザの他のユーザ識別情報（ユーザＩＤ及びパスワード）が含まれる。

【００５４】このように個人情報３１０が前述のディレクトリ標準Ｘ．５００にしたがって管理される場合、上記識別情報要求ステップＳ１０２においては、認証オブジェクト８１は、例えば上記ディレクトリ標準で定められたユーザの識別情報である識別名（ＤＮ）の入力をクライアントプログラム６１に要求する。ユーザが自己の識別名（ＤＮ）を入力すると、クライアントプログラム６１が入力されたユーザ識別名（ＤＮ）を認証オブジェクト８１に引き渡す（ステップＳ１０３）。

【００５５】認証オブジェクト８１は、入力された識別名（ＤＮ）を有する個人情報をディレクトリサーバプログラム３１から取得する（ステップＳ１０４）。認証オブジェクト８１は、取得された個人情報を用いて高度の安全性を有する認証プロトコルに基づいてクライアントプログラム６１と通信してユーザの認証を行う（ステップＳ１０５）。このときクライアントプログラム６１も適宜応答する（ステップＳ１０６）。上記認証プロトコルには例えばチャレンジ応答プロトコルを使用することができる。

【００５６】アクセス管理サーバプログラム１００は、上記個人認証において上記認証プロトコルに代えて、上記ユーザＩＤとパスワードを用いた認証も行ってもよいが、上記認証プロトコルを用いることにより、通信の傍受等を防止することができ、より安全に個人認証を行うことができる。

【００５７】ユーザが個人認証に合格しなかった場合（ステップＳ１０７）、認証オブジェクト８１は、アクセス拒否をクライアントプログラム６１に通知する（ステップＳ１０８）。一方、ユーザが認証に合格すると（ステップＳ１０７）、認証オブジェクト８１は、ファクトリ起動オブジェクト８２を呼び出す（ステップＳ１０９）。このとき、認証オブジェクト８１は、ユーザの個人情報３１０に含まれたアクセスレベルと前述の他のユーザ識別情報（ユーザＩＤとパスワード）をファクトリ起動オブジェクト８２に引き渡す。

【００５８】図７は、ファクトリ起動オブジェクト８２の例を模式的に示す。ファクトリ起動オブジェクト８２は、メソッドとしてファクトリロードメソッド８２Ａとロード済みファクトリ更新メソッド８２Ｂを含み、属性値としてロード済みファクトリテーブル８２０を含む。ロード済みファクトリテーブル８２０は、各アクセスレベルに対応するファクトリがメモリ１１にロード済みか否かを示すテーブルである。

【００５９】図８は、ロード済みファクトリテーブル８２０の例を示す。ロード済みファクトリテーブル８２０には、各アクセスレベルに対応して、アクセスレベルを記憶する領域８２１と、対応するファクトリの参照値を記憶する領域８２２が設けられる。あるアクセスレベルに対応するファクトリがメモリ１１にロードされたときには、当該アクセスレベルに対応して当該ファクトリの参照値が参照値記憶領域８２２に記憶される。しかし、そのアクセスレベルに対応するファクトリがメモリ１１にロードされていないときには、当該アクセスレベルに対応する参照値記憶領域８２２には、それ以外の値、例えば「０」が記憶されたままである。

【００６０】図では、アクセスレベル「１」と「３」に対しては対応するファクトリが既にロードされ、当該ファクトリの参照値を例示する値「ＡＡＡＡ」と「ＢＢＢＢ」が記憶され、アクセスレベル「２」と「４」に対しては対応するファクトリがロードされていないことを示す値「０」が参照値記憶領域８２２に記憶されている。

【００６１】図４において、ファクトリ起動オブジェクト８２は、認証オブジェクト８１により呼び出されると、ファクトリロードメソッド８２Ａを起動する。このファクトリロードメソッド８２Ａは、ロード済みファクトリテーブル８２０を参照して認証オブジェクト８１より通知されたユーザのアクセスレベルに対応するファクトリがメモリ１１にロード済みであるか否かを判別する（ステップＳ１１０）。

【００６２】もしそのファクトリがまだメモリ１１にロードされていないと判断されたときには（ステップＳ１１１）、ディレクトリサーバプログラム３１（図１）が

管理するファクトリテーブル３１Ｂから、当該ファクトリをメモリ１１にロードし（ステップＳ１１２）、ロードされたファクトリの参照値をファクトリテーブル８２０（図８）内のユーザのアクセスレベルに対応する参照値記憶領域８２２にセットする（ステップＳ１１３）。

【００６３】その後、当該ファクトリ８４を呼び出す（ステップＳ１１４）。このとき、ファクトリ起動オブジェクト８２は、前述の他のユーザ識別情報（ユーザＩＤとパスワード）を当該ファクトリに引き渡す。一方、ステップＳ１１１において、ユーザのアクセスレベルに対応するファクトリ８４が既にメモリ１１にロード済みであると判断された場合には、ステップＳ１１２からＳ１１３は実行されず、ステップＳ１１４が実行される。

【００６４】図９は、ファクトリ８４の例を模式的に示す。ファクトリ８４は、メソッドとしてアクセスオブジェクト生成メソッド８４Ａと対応するアクセスレベルのユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムをそれぞれアクセスするための一つ又は複数のアクセスメソッド（今の例では複数のアクセスメソッド８４Ｂ、８４Ｃ）を含む。

【００６５】アクセスメソッド８４Ｂ、８４Ｃは、それぞれの属性値として対応する機密情報管理サーバプログラムと通信するための通信制御情報を含む。通信制御情報には、例えば当該機密情報管理サーバプログラムが実装されたコンピュータノードのＩＰアドレスと当該コンピュータノード内のポート番号と当該コンピュータノードと通信するための通信用デバイスドライバの名称が含まれている。

【００６６】ファクトリ８４は、オブジェクト属性値としてアクセスレベル８４１、アクセスイネーブルリスト８４２、アクセスディスエーブルリスト８４３を更に含む。アクセスレベル８４１は、当該ファクトリが対応するアクセスレベルを示し、アクセスイネーブルリスト８４２は、当該アクセスレベルのユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムを示す。アクセスディスエーブルリスト８４３は、当該アクセスレベルのユーザがアクセス権限を有しない一つ又は複数の機密情報管理サーバプログラムを示す。

【００６７】図にはこれらの属性の値の例を括弧内に示している。アクセスレベル８４１が例えば「２」であり、アクセスイネーブルリスト８４２は、ユーザがアクセス権限を有する機密情報管理サーバプログラムとして機密情報管理サーバプログラム＃１（２０Ａ）と機密情報管理サーバプログラム＃３（２２Ａ）を示し、アクセスディスエーブルリスト８４３は、ユーザがアクセス権限を有しない機密情報管理サーバプログラムとして機密情報管理サーバプログラム＃２（２１Ａ）を示している。

【００６８】図４に戻り、ファクトリ８４は、ファクトリ起動オブジェクト８２により呼び出されると、アクセスオブジェクト生成メソッド８４Ａを実行し、当該メソッドによりユーザ用のアクセスオブジェクト８５を生成する（ステップＳ１１５）。

【００６９】図１０は、アクセスオブジェクト８５の例を模式的に示す。アクセスオブジェクト８５は、メソッドとしてユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムをそれぞれアクセスするための一つ又は複数のアクセスメソッド（今の例では複数のアクセスメソッド８５Ａ、８５Ｂ）を含む。これらのアクセスメソッド８５Ａ、８５Ｂは、ファクトリ８４内のアクセスメソッド８４Ｂ、８４Ｃと同じである。

【００７０】すなわち、ファクトリ８４のアクセスオブジェクト生成メソッド８４Ａは、ステップＳ１１５においてアクセスオブジェクト８５を生成するときに、ファクトリ８４内のメソッド８４Ｂ、８４Ｃをアクセスオブジェクト８５内にコピーしてアクセスオブジェクト８５内のアクセスメソッド８５Ａ、８５Ｂを生成する。したがって、アクセスメソッド８５Ａ、８５Ｂは、それぞれの属性値としてアクセスメソッド８４Ｂ、８４Ｃの属性値と同じ通信制御情報を含む。

【００７１】アクセスオブジェクト８５は、オブジェクトの属性値としてアクセスレベル８５１、アクセスイネーブルリスト８５２、アクセスディスエーブルリスト８５３、ユーザＩＤとパスワード８５４を更に含む。アクセスレベル８５１、アクセスイネーブルリスト８５２、アクセスディスエーブルリスト８５３は、ファクトリ８４の属性値８４１から８４３（図９）と同じである。

【００７２】すなわち、ファクトリ８４のアクセスオブジェクト生成メソッド８４Ａは、ステップＳ１１５（図４）においてアクセスオブジェクト８５を生成するときに、ファクトリ８４内のアクセスレベル８４１、アクセスイネーブルリスト８４２、アクセスディスエーブルリスト８４３をアクセスオブジェクト８５内にコピーする。属性値としてのユーザＩＤとパスワード８５４には、ファクトリ起動オブジェクト８２からファクトリ８４に引き渡された引数が使用される。

【００７３】図４に戻り、起動されたファクトリ８４は、生成されたアクセスオブジェクト８５の参照値をファクトリ起動オブジェクト８２に戻す（ステップＳ１１６）。ファクトリ起動オブジェクト８２は、認証オブジェクト８１にアクセスオブジェクト８５の参照値を戻す（ステップＳ１１７）。

【００７４】図５を参照するに、認証オブジェクト８１は、コンテンツ生成オブジェクト８３を呼び出し、引数としてアクセスオブジェクト８５の参照値を引き渡す（ステップＳ１１８）。コンテンツ生成オブジェクト８３は、コンテンツオブジェクト８６を生成し（ステップＳ１１９）、生成されたコンテンツオブジェクト８６の参照値を認証オブジェクト８１に戻す（ステップＳ１２０）。

【００７５】図１１は、コンテンツ生成オブジェクト８３の例を模式的に示す。コンテンツ生成オブジェクト８３は、メソッドとしてコンテンツ生成メソッド８３Ａと、メインメニューリスト提供メソッド８３Ｂと、複数の機密情報サービス利用メソッド８３Ｃ、８３Ｄ、…とを含み、属性値としてメインメニューリストデータ８３１を含む。

【００７６】機密情報サービス利用メソッド８３Ｃ、８３Ｄ、…は、本コンピュータシステムで利用可能な複数の機密情報管理サーバプログラム＃１（２０Ａ）、＃２（２１Ａ）、＃３（２２Ａ）（図１）により提供される全機密情報サービスのいずれかを利用するためのメソッドである。メインメニューリストデータ８３１は、これらの全機密情報サービスの名称等をクライアントプログラム６１に提示するためのデータである。

【００７７】図１２は、メインメニューリストデータ８３１の例を示す。メインメニューリストデータ８３１は、機密情報サービスの名称８３１Ａと機密情報サービス利用メソッド名８３１Ｂとの対を本コンピュータシステムで利用可能な全機密情報サービスに対して含む。機密情報サービス利用メソッド名８３１Ｂには、コンテンツ生成オブジェクト８３（図１１）に含まれた機密情報サービス利用メソッド８３Ｃ、８３Ｄ、…のうち記憶領域８３１Ａに記憶された機密情報サービスの名称に対応するメソッドの名称が使用される。

【００７８】例えば機密情報サービスの名称として「勤休表登録」が含まれ、コンテンツ生成オブジェクト８３内に含まれた対応する機密情報サービス利用メソッドの名称として「勤休表登録メソッド」が含まれる。このメインメニューリストデータ８３１の使用方法は後に説明する。

【００７９】図１３は、コンテンツオブジェクト８６の例を模式的に示す。コンテンツオブジェクト８６は、メソッドとしてメインメニューリスト提供メソッド８６Ａと、複数の機密情報サービス利用メソッド８６Ｂ、８６Ｃ、…とを含み、属性値としてメインメニューリストデータ８６１を含む。メインメニューリスト提供メソッド８６Ａ、機密情報サービス利用メソッド８６Ｂ、８６Ｃ、…は、コンテンツ生成オブジェクト８３内のメソッド８３Ｂ、８３Ｃ、８３Ｄ、…と同じである。

【００８０】コンテンツ生成オブジェクト８３は、認証オブジェクト８１から呼ばれると、コンテンツ生成メソッド８３Ａを実行する。前述のステップＳ１１９及びＳ１２０はコンテンツ生成メソッド８３Ａにより実行される。コンテンツ生成メソッド８３Ａは、ステップＳ１１９においてコンテンツオブジェクト８６を生成するときに、コンテンツ生成オブジェクト８３内のメソッド８３Ｂ、８３Ｃ、８３Ｄ、…をコンテンツオブジェクト８６内にコピーしてコンテンツオブジェクト８６内のメソッド８６Ａ、８６Ｂ、８６Ｃ、…を生成する。

【００８１】同様に、コンテンツ生成オブジェクト８３内のメインメニューリストデータ８３１をコピーしてコンテンツオブジェクト８６内の属性値としてメインメニューリストデータ８６１を生成する。更にコンテンツ生成オブジェクト８３は、アクセスオブジェクト８５の参照値８６２をコンテンツオブジェクト８６の属性値として組み込む。コンテンツ生成メソッド８３Ａは、その後、コンテンツオブジェクト８６の参照値を認証オブジェクト８１に戻すステップＳ１２０を実行する。

【００８２】図５に戻り、認証オブジェクト８１は、オブジェクトアダプタ８７（図１）を呼び出し、コンテンツオブジェクト８６の参照値を引き渡してオブジェクトレファレンスの生成を要求する（ステップＳ１２１）。オブジェクトアダプタ８７からコンテンツオブジェクト８６のオブジェクトレファレンスを受け取り（ステップＳ１２２）、クライアントプログラム６１にこのオブジェクトレファレンスを戻す（ステップＳ１２３）。

【００８３】図６において、クライアントプログラム６１は、戻されたオブジェクトレファレンスを用いてコンテンツオブジェクト８６を呼び出す（ステップＳ１２４）。コンテンツオブジェクト８６は、クライアントプログラム６１から呼び出されると、メインメニューリスト提供メソッド８６Ａ（図１３）を起動する。起動されたメインメニューリスト提供メソッド８６Ａは、メインメニューリストデータ８６１をクライアントプログラム６１に戻す（ステップＳ１２５）。

【００８４】クライアントプログラム６１は、戻されたメインメニューリストデータ８６１に基づいて、図１４に例示するように、そこに含まれた機密情報サービスの名称の一覧をメインメニューとして表示装置の画面に表示する（ステップＳ１２６）。ユーザが表示されたいずれかの機密情報サービスの名称を選ぶと、クライアントプログラム６１は、その名称のサービスを利用するためのメソッドを呼び出す（ステップＳ１２７）。具体的には、クライアントプログラム６１は、ユーザが選択した機密情報サービスの名称に対応してメインメニューリストデータ８６１に含まれた機密情報サービス利用メソッドの名称を指定してコンテンツオブジェクト８６を呼び出す。

【００８５】コンテンツオブジェクト８６では、指定された名称の機密情報サービス利用メソッド、例えば８６Ｂが起動され、この機密情報サービス利用メソッドが、アクセスオブジェクト８５の参照値８６２（図１３）を用いてアクセスオブジェクト８５を呼び出し、当該機密情報サービス利用メソッドに対応して定められた、当該機密情報サービス利用メソッドが利用する機密情報サービスを提供する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを呼び出す（ステップＳ１２８）。

【００８６】例えば、ユーザが機密情報サービスとして

勤休表登録を選んだ場合、コンテンツオブジェクト８６内の当該サービスを利用するためのメソッド、例えば８６Ｂ（図１３）が起動され、起動されたメソッド８６Ｂは、当該機密情報サービスを提供する機密情報管理サーバプログラム、例えば２０Ａ（図1）にアクセスするためのアクセスメソッド、例えば８５Ａ（図１０）を呼び出す。

【００８７】アクセスオブジェクト８５は、呼び出されたアクセスメソッド８５Ａが内部に存在するか否かを判断し（ステップＳ１２９）、そのアクセスメソッドが存在する場合には、当該呼び出しを受け付ける、すなわちユーザのアクセス要求を受け付ける。すなわちそのアクセスメソッドの属性値である通信制御情報に含まれたＩＰアドレス、ポート番号、通信用のデバイスドライバを用いて当該機密情報管理サーバプログラム、例えば２０Ａにアクセスする。

【００８８】こうしてクライアントプログラム６１と当該機密情報管理サーバプログラム２０Ａとの間で、コンテンツオブジェクト８６内の機密情報サービス利用メソッド８６Ｂ及びアクセスオブジェクト８５内のアクセスメソッド、例えば８５Ａを経由した通信路が形成される。

【００８９】上記アクセスメソッド８５Ａは、機密情報管理サーバプログラム２０Ａからユーザ識別情報の入力を求められたときには、アクセスオブジェクト８５の属性値として記憶された前述のユーザ識別情報（ユーザＩＤとパスワード）８５４（図１０）をユーザに代わって機密情報管理サーバプログラム２０Ａに送信する。

【００９０】機密情報管理サーバプログラム２０Ａによる個人認証が成功すると、上記アクセスメソッド８５Ａは、当該機密情報管理サーバプログラムからの戻り値（応答情報）をコンテンツオブジェクト８６内の機密情報サービス利用メソッド８６Ｂに戻す（ステップＳ１３０）。当該機密情報サービス利用メソッド８６Ｂは、戻り値をクライアントプログラム６１に戻す（ステップＳ１３２）。

【００９１】その後、ユーザがクライアントプログラム６１に機密情報サービスを利用するためのデータを入力すると、当該データは、コンテンツオブジェクト８６内の上記機密情報サービス利用メソッド８６Ｂ及びアクセスオブジェクト８５内の上記アクセスメソッド８５Ａを経由して上記機密情報管理サーバプログラム２０Ａに転送され、再度機密情報管理サーバプログラム２０Ａから戻り値が上記通信路を経てクライアントプログラム６１に戻される。

【００９２】このようにして、ユーザはクライアントプログラム６１を介してアクセス権限を有する機密情報管理サーバプログラムが提供する機密情報サービスを利用することができる。ユーザによる機密情報サービスの利用が終了するとアクセス管理サーバプログラム１００及びクライアントプログラム６１の処理が終了する。ユーザによるいずれかの機密情報管理サーバプログラムの使用が終了すると、当該ユーザ用のアクセスオブジェクト８５及びコンテンツオブジェクト８６はメモリ１１から削除される。

【００９３】ステップＳ１２８によりアクセスオブジェクト８５内のアクセスメソッドがコンテンツオブジェクト８６内の機密情報サービス利用メソッドにより呼び出されたときに、当該アクセスメソッドがアクセスオブジェクト８５内に存在しない場合（ステップＳ１２９）、アクセスオブジェクト８５は、当該呼び出しを受け付けない、すなわちユーザのアクセス要求を受け付けない。

【００９４】具体的には、アクセスオブジェクト８５は、ユーザが選択した機密情報サービスを利用できない旨をコンテンツオブジェクト８６内の呼び出し元の機密情報サービス利用メソッドに戻す（ステップＳ１３１）。当該機密情報サービス利用メソッドは、その戻り値をクライアントプログラム６１に戻し（ステップＳ１３２）、アクセス管理サーバプログラム１００の処理が終了する。こうしてユーザがアクセス権限を有しない機密情報管理サーバプログラムへのアクセスは禁止される。

【００９５】このようにユーザに対応してアクセスオブジェクト８５及びコンテンツオブジェクト８６が生成され、これらのオブジェクトを用いてユーザのアクセス権限の有無、すなわちアクセス要求がユーザがアクセス権限を有する機密情報に対するものであるかが判断される。ユーザがアクセス権限を有する場合、これらのオブジェクトを用いてユーザが要求した機密情報を管理する機密情報管理サーバプログラムとユーザが利用するクライアントプログラムの間で通信路が形成される。

【００９６】したがって、各ユーザによる機密情報へのアクセス権限のチェックとアクセスが、他のユーザに対する同様の処理と独立にかつ並行に実行される。その結果、各ユーザのアクセス権限のチェックとアクセスを他のユーザに対する同様の処理の影響を受けないで効率よく実行できる。

【００９７】なお、アクセスポリシーあるいはシステム構成の変更が生じたとき、アクセス管理サーバプログラム１００がコンピュータノード４０を用いてシステム管理者により以下のようにして更新される。

【００９８】システム管理オブジェクト４１には、アクセスポリシーを示すアクセスポリシー表及び機密情報管理サーバプログラムの構成を示すシステム構成表を属性値として含んでいる。

【００９９】図１５は、アクセスポリシー表４０１の例を示す。アクセスポリシー表４０１は、使用可能なアクセスレベルの各々に対して、当該アクセスレベルのユーザが各機密情報管理サーバプログラムに対してアクセス権限を有する否かのフラグを保持している。図ではフラ

グ値「１」がアクセス権限があることを示し、「０」がアクセス権限がないことを示す。

【０１００】例えば、アクセスレベル「１」のユーザは、機密情報管理サーバプログラム＃１から＃３のいずれに対してアクセス権限を有するが、アクセスレベル「２」のユーザは、機密情報管理サーバプログラム＃１と＃３に対してアクセス権限を有し、機密情報管理サーバプログラム＃２に対してはアクセス権限を有しないことが示されている。

【０１０１】なお、アクセスポリシーの変更態様には、あるアクセスレベルに対するアクセス権限が変更される場合がある。あるアクセスレベル自体が削除される場合もある。さらにはアクセスレベルが追加される場合もある。

【０１０２】図１６は、システム構成表４０２の例を示す。システム構成表４０２は、使用可能な機密情報管理サーバプログラムの各々に対して当該機密情報管理サーバプログラムにアクセスするために使用される通信制御情報を保持している。通信制御情報には、例えば当該機密情報管理サーバプログラムが実装されたコンピュータノードのＩＰアドレスと当該コンピュータノード内のポート番号と当該コンピュータノードと通信するための通信用デバイスドライバの名称が含まれている。

【０１０３】システム構成の変更態様には、ある機密情報管理サーバプログラムが変更される場合、すなわち、当該機密情報管理サーバプログラムの通信制御情報が変更される場合がある。あるいは機密情報管理サーバプログラムが削除される場合もある。さらには機密情報管理サーバプログラムが追加される場合もある。

【０１０４】図１７はシステム管理オブジェクト４１の処理の一例の概略フローチャートを示す。システム管理オブジェクト４１は、システム管理者により起動されると、システム管理者の要求に応じて上記アクセスポリシー表４０１及びシステム構成表４０２を表示装置の画面に表示し、アクセスポリシーとシステム構成の変更入力を受け付け（ステップＳ４１１）、削除するべきファクトリ及び追加するべきファクトリを指定してファクトリ更新オブジェクト４２にそれぞれのファクトリの削除又は追加を要求する（ステップＳ４１２）。

【０１０５】削除するべきファクトリと追加すべきファクトリは変更入力に基づいて判別される。既にあるファクトリが新たなファクトリにより置換されるべきときには、元のファクトリの削除と新たなファクトリの追加が必要となる。なお、追加するべきファクトリは、システム管理者により本コンピュータシステムとは別のところで事前に生成してコンピュータノード４０内に記憶させておき、後にファクトリの更新を実行するときに当該追加すべきファクトリをファクトリテーブル３１Ｂに移動すればよい。しかし、追加すべきファクトリをシステム管理オブジェクト４１により自動的に生成させることがより望ましい。

【０１０６】アクセスポリシーの変更態様とファクトリの更新態様との関係は以下のとおりである。あるアクセスレベルのアクセス権限が変更されたときには、当該アクセスレベルを有するユーザに対して生成するアクセスオブジェクト８５（図１０）内に含まれるアクセスメソッド及び属性値を変更する必要がある。したがって、当該アクセスオブジェクトの生成に用いる、当該アクセスレベルに対応するファクトリを新たなファクトリにより置換する必要がある。

【０１０７】あるアクセスレベル自体が削除された場合には、当該アクセスレベルに対応するファクトリを削除する必要がある。あるアクセスレベルが追加された場合には、当該アクセスレベルに対応するファクトリを追加する必要がある。

【０１０８】システム構成の変更態様とファクトリの更新態様との関係は以下のとおりである。ある機密情報管理サーバプログラムが変更されたとき、すなわち、当該機密情報管理サーバプログラムの通信制御情報が変更されたときには、当該機密情報管理サーバプログラムに対するアクセス権限を有するアクセスレベルに対応するファクトリをすべて新たなファクトリにより置換する必要がある。あるいは機密情報管理サーバプログラムが削除された場合もあるいは新たに追加された場合も同様である。

【０１０９】図１８は、ファクトリ更新オブジェクト４２の処理の一例の概略フローチャートを示す。ファクトリ更新オブジェクト４２は、システム管理オブジェクト４１により起動されると、ディレクトリサーバプログラム３１内のファクトリテーブル３１Ｂに含まれたファクトリを更新する、すなわち、ファクトリを削除するか又はそこに新たなファクトリをコンピュータノード４０から追加する（ステップＳ４２１）。

【０１１０】その後、ファクトリ更新オブジェクト４２は、システム構成の変更がなされたか否かを判断する（ステップＳ４２２）。システム構成の変更がなされた場合には、後に説明するようにメインオブジェクト８０を新たなメインオブジェクトにより置換し、当該新たなメインオブジェクトを再起動する必要がある。その場合には、メモリ１１にロード済みのファクトリ等はすべて削除されるので、以下に述べる処理は実行されず、ファクトリ更新オブジェクト４２は終了する。

【０１１１】ステップＳ４２２においてシステム構成の変更がないと判断された場合には、ファクトリ起動オブジェクト８２内のロード済みファクトリ更新メソッド８２Ｂ（図７）にロード済みのファクトリの一部の削除とロード済みファクトリテーブル８２０の更新を要求する（ステップＳ４２３）。

【０１１２】削除されるべきファクトリは、ディレクトリサーバプログラム３１内のファクトリテーブル３１Ｂ

から削除されたファクトリのうちメモリ１１にロード済みのファクトリである。すなわち、新たなファクトリにより置換されるべきファクトリ又は不要になったファクトリであって、メモリ１１にロード済みのファクトリである。ファクトリ起動オブジェクト８２内のロード済みファクトリ更新メソッド８２Ｂは、指定されたファクトリをメモリ１１から削除する。

【０１１３】更に、ロード済みファクトリ更新メソッド８２Ｂは、当該削除されたファクトリに対するアクセスレベルが削除されていない場合には、ロード済みファクトリテーブル８２０（図８）の、上記削除されたファクトリに対応するアクセスレベルに対する参照値記憶領域８２２に値「０」を記憶する。アクセスレベルが削除された場合には、ロード済みファクトリテーブル８２０内の当該アクセスレベルに対応する参照値記憶領域８２２にアクセスレベルの削除を示す値、例えば「－１」を記憶する。あるいは、ロード済みファクトリテーブル８２０内の当該アクセスレベルを記憶する領域８２１と、対応する参照値記憶領域８２２を削除してもよい。

【０１１４】アクセスレベルが追加された場合には、ロード済みファクトリテーブル８２０内に当該アクセスレベルを記憶する領域８２１と、対応する参照値記憶領域８２２を追加し、追加された領域８２１に追加されたアクセスレベルを記憶し、追加された参照値記憶領域８２２に、ロードされていないことを示す値「０」を格納する。こうしてファクトリ更新オブジェクト４２は終了する。

【０１１５】図１７に戻り、システム管理オブジェクト４１は、ファクトリ更新オブジェクト４２による処理が終了すると、システム構成の変更がなされたか否かを判断する（ステップＳ４１３）。システム構成の変更がなされていないときには、システム管理オブジェクト４１は終了する。

【０１１６】こうして、ファクトリ起動オブジェクト８２は、アクセスポリシーの変更後も、メモリ１１にロードされていないファクトリをディレクトリサーバプログラム３１内のファクトリテーブル３１Ｂから、アクセスしてきたユーザのアクセスレベルに対応するファクトリをロードするだけでよいことになる。

【０１１７】一方、ステップＳ４１３においてシステムの構成が変更されたと判断されたときには、後に述べる理由により使用中のメインオブジェクト８０を新たなメインオブジェクトにより置換し、当該新たなメインオブジェクトを再起動する（ステップＳ４１４）。当該新たなメインオブジェクトは、システム管理者が事前にコンピュータノード４０内に準備しておけばよい。しかし、システム管理オブジェクト４１により新たなメインオブジェクトを自動的に生成することがより望ましい。

【０１１８】新たなメインオブジェクトが再起動されると、使用中であった認証オブジェクト８１、ファクトリ起動オブジェクト８２、コンテンツ生成オブジェクト８３、ロード済みのファクトリ８４、生成済みのアクセスオブジェクト８５、コンテンツオブジェクト８６は削除され、新たに認証オブジェクト８１、ファクトリ起動オブジェクト８２、コンテンツ生成オブジェクト８３が生成される。

【０１１９】メインオブジェクトの更新と再起動が必要な理由は以下のとおりである。システム構成の変更に伴い、利用可能な機密情報サービスが変更される。例えば、機密情報管理サーバプログラムが追加された場合には、その機密情報管理サーバプログラムにより提供される機密情報サービスを利用するために新たな機密情報サービス利用メソッドをコンテンツ生成オブジェクト８３内のメソッドとして追加することが必要となる。併せてメインメニューリストデータ８３１の内容も増やすことが必要になる。

【０１２０】あるいは、システム構成の変更に伴い、既に利用可能な機密情報サービスが他の機密情報サービスにより置換された場合、当該既にあった古い機密情報サービスを利用するための、コンテンツ生成オブジェクト８３内に含まれていた特定の機密情報サービス利用メソッドを新たな機密情報サービス利用メソッドにより置換する必要が生じる。併せて、メインメニューリストデータ８３１内の当該古い機密情報サービスに関連するデータを新たな機密情報サービスに関連するデータで置換する必要が生じる。

【０１２１】したがって、システム構成が変更されたときには、使用中のコンテンツ生成オブジェクト８３及びそこから生成されたコンテンツオブジェクト８６を更新する必要がある。コンテンツオブジェクト８６は、コンテンツ生成オブジェクト８３により生成され、コンテンツ生成オブジェクト８３は、メインオブジェクト８０により生成されるので、メインオブジェクト８０自体を更新する必要がある。

【０１２２】以上のようにして、アクセスポリシーの更新及びシステム構成の変更時にアクセス管理サーバプログラム１００をシステム管理者の制御の元で更新することができる。

【０１２３】このようにアクセス管理サーバプログラム１００が使用するファクトリ８４をディレクトリサーバプログラム３１に格納し、アクセス管理サーバプログラム１００がディレクトリサーバプログラム３１からアクセス管理サーバプログラム１００が使用するメモリ１１にロードする方法を採ると、アクセスポリシーあるいはシステム構成の変更にアクセス管理サーバプログラム１００を適合させるために必要なアクセス管理サーバプログラム１００の変更量が少なくなる。このことは、複数のアクセス管理サーバプログラムが異なるコンピュータノードに実装されている場合に特に有効である。

【０１２４】上記実施の形態では、個人情報と複数のフ

ァクトリをディレクトリサーバプログラム３１により記憶された。このことは、以下の点で優れている。ディレクトリサーバプログラムは極めて容易にバイナリデータを保持することができる。したがって、ディレクトリサーバプログラム３１は、バイナリデータである複数のファクトリを保持するのに適している。更に、企業の個人情報群は基本的には階層構造を有している。元々ディレクトリサーバプログラム３１は情報をツリー構造を用いて階層構造で保存する。したがって、ディレクトリサーバプログラムは、個人情報群を階層的に保存するのに適している。

【０１２５】更に、ディレクトリサーバプログラム３１は、電子証明書を含む個人情報を記憶しており、高度のセキュリティ機能を有する認証アルゴリズムにしたがって、アクセス管理サーバプログラム１００のための個人認証を行うことができる。しかも、最近は多くの企業で個人情報をディレクトリサーバプログラムにより管理している。本実施の形態は、そのようなディレクトリサーバプログラムをファクトリの記憶にも共用しているので、新たなディレクトリサーバプログラムを使用しないで実現することができる。

【０１２６】なお、本発明は以上の実施の形態に限定されないことは言うまでもない。例えば、コンテンツ生成オブジェクト８３及びコンテンツオブジェクト８６に使用されたメインメニューリストデータ８３１（図１１）又は８６１（図１３）は、提供される機密情報サービスのすべてに関する機密情報サービスの名称等を含んでいた。

【０１２７】しかし、コンテンツオブジェクト８６に含まれるメインメニューリストデータ８６１として、ユーザのアクセスレベルに対してアクセス権限が与えられない機密情報サービスに対するデータを含まないものを用いることもできる。このようなメインメニューリストデータは、あらかじめアクセスレベルに対応して生成しておけばよい。この場合には、ユーザにアクセス権限がない機密情報サービスをユーザが選択することはなくなる。このことにより当該機密情報サービスに対するユーザのアクセス要求を受け付けないようにしていることになる。

【０１２８】また、認証オブジェクト８１による個人認証ではディレクトリ標準Ｘ．５００により定められた識別名（ＤＮ）を用いたが、これに代えてユーザ認証情報とパスワードを用いて個人認証を行ってもよい。更に、機密情報管理サーバプログラム２０Ａを内蔵するコンピュータノード２０等は、ＬＡＮ７０により接続された、企業等の団体の内部で使用されるものが例示されたが、当該コンピュータノード２０等は、インターネットあるいは専用回線等で接続された遠方に位置するものでもよく、また、機密情報も企業等の団体内の個人に関する情報でなくてもよいことは言うまでもない。

【０１２９】

【発明の効果】以上に説明したように、本発明によればアクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時に、その変更にアクセス管理プログラムを比較的簡単に適合させることができる。

【図面の簡単な説明】

【図１】本発明に係るアクセスプログラムの一つの実施の形態を使用するコンピュータの概略構成図である。

【図２】アクセス管理サーバプログラムにより実行される一例としての処理の流れを模式的に示す図である。

【図３】アクセス管理サーバプログラムにより実行される一例としての処理の流れの一部の概略フローチャートである。

【図４】アクセス管理サーバプログラムにより実行される一例としての処理の流れの他の一部の概略フローチャートである。

【図５】アクセス管理サーバプログラムにより実行される一例としての処理の流れの更に他の一部の概略フローチャートである。

【図６】アクセス管理サーバプログラムにより実行される一例としての処理の流れの更に他の一部の概略フローチャートである。

【図７】ファクトリ起動オブジェクトの例を模式的に示す図である。

【図８】ロード済みファクトリテーブルの例を示す図である。

【図９】ファクトリの例を模式的に示す図である。

【図１０】アクセスオブジェクトの例を模式的に示す図である。

【図１１】コンテンツ生成オブジェクトの例を模式的に示す図である。

【図１２】メインメニューリストデータの例を模式的に示す図である。

【図１３】コンテンツオブジェクトの例を模式的に示す図である。

【図１４】ユーザに対して表示される機密情報サービスの名称の一覧の例を示す図である。

【図１５】アクセスポリシー表の例を示す図である。

【図１６】システム構成表の例を示す図である。

【図１７】システム管理オブジェクトの処理の一例の概略フローチャートである。

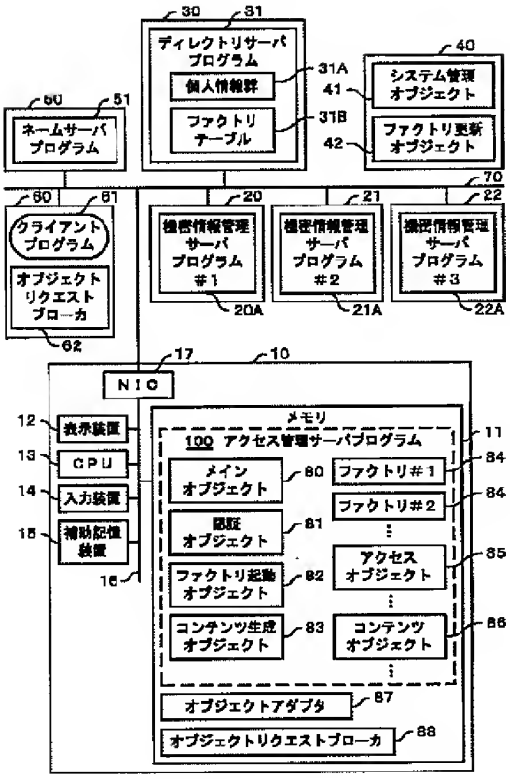
【図１８】ファクトリ更新オブジェクトの処理の一例の概略フローチャートである。

【符号の説明】

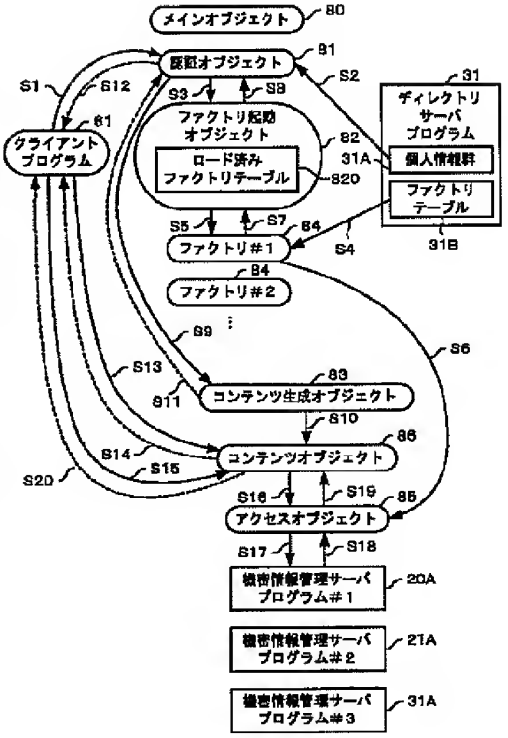
１０、２０、２１、２２、３０、４０、５０、６０…コンピュータノード

７０…ＬＡＮ

【図１】



【図２】



【図１４】

【図７】

82 ファクトリ起動オブジェクト

メソッド	ファクトリロードメソッド	82A
	ロード済みファクトリ更新メソッド	82B
属性値	ロード済みファクトリテーブル	820

【図８】

820 ロード済みファクトリテーブル

アクセスレベル (821)	参照値 (822)
1	AAAA
2	0
3	BBBB
4	0
⋮	⋮

【図９】

84 ファクトリ

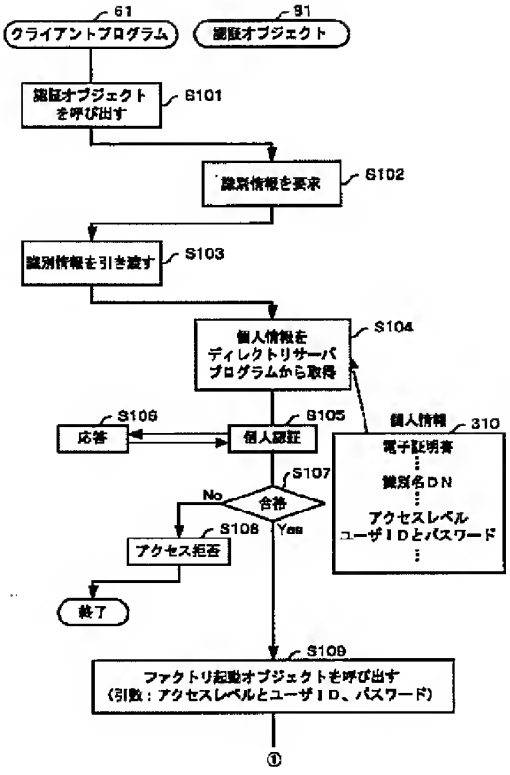
メソッド	アクセスオブジェクト生成メソッド	84A
	アクセスメソッド(機密情報管理サーバプログラム#1用) メソッド属性値：通信制御情報	84B
	アクセスメソッド(機密情報管理サーバプログラム#3用) メソッド属性値：通信制御情報	84C
属性値	アクセスレベル（2）	841
	アクセスイネーブルリスト（1，3）	842
	アクセスディスエーブルリスト（2）	843

【図１０】

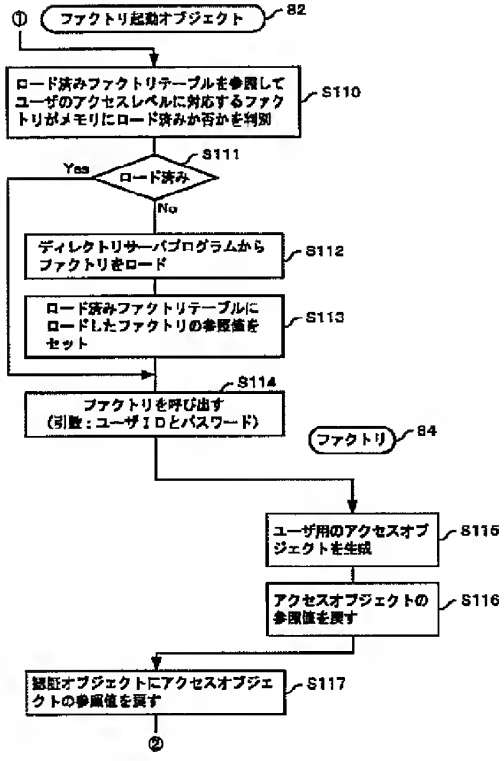
85 アクセスオブジェクト

メソッド	アクセスメソッド(機密情報管理サーバプログラム#1用) メソッド属性値：通信制御情報	85A
	アクセスメソッド(機密情報管理サーバプログラム#3用) メソッド属性値：通信制御情報	85B
属性値	アクセスレベル（2）	851
	アクセスイネーブルリスト（1，3）	852
	アクセスディスエーブルリスト（2）	853
	ユーザＩＤとパスワード	854

【図３】



【図４】



【図１１】

63 コンテンツ生成オブジェクト

メソッド	コンテンツ生成メソッド	63A
	メインメニューリスト提供メソッド	63B
	機密情報サービス利用メソッド1	63C
	機密情報サービス利用メソッド2	63D
	⋮	
属性値	メインメニューリストデータ	831

【図１２】

831 メインメニューリストデータ

831A	831B
機密情報サービス名	機密情報サービス利用メソッド名
勤休表登録	勤休表登録メソッド
⋮	⋮

【図１３】

86 コンテンツオブジェクト

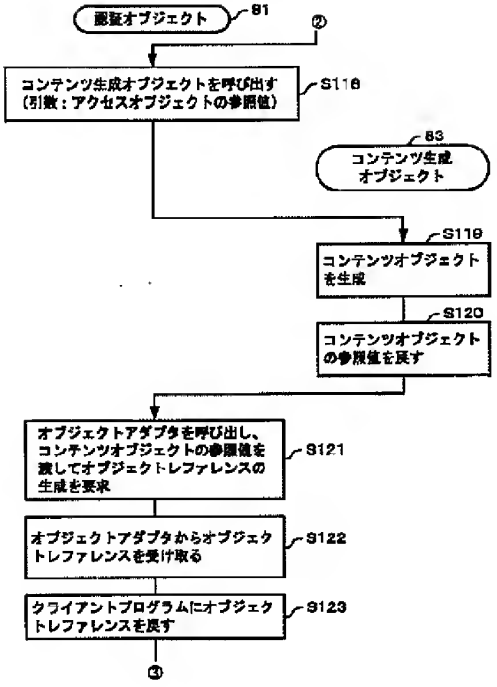
メソッド	メインメニューリスト提供メソッド	86A
	機密情報サービス利用メソッド1	86B
	機密情報サービス利用メソッド2	86C
	⋮	
属性値	メインメニューリストデータ	861
	アクセスオブジェクトの参照値	862

【図１５】

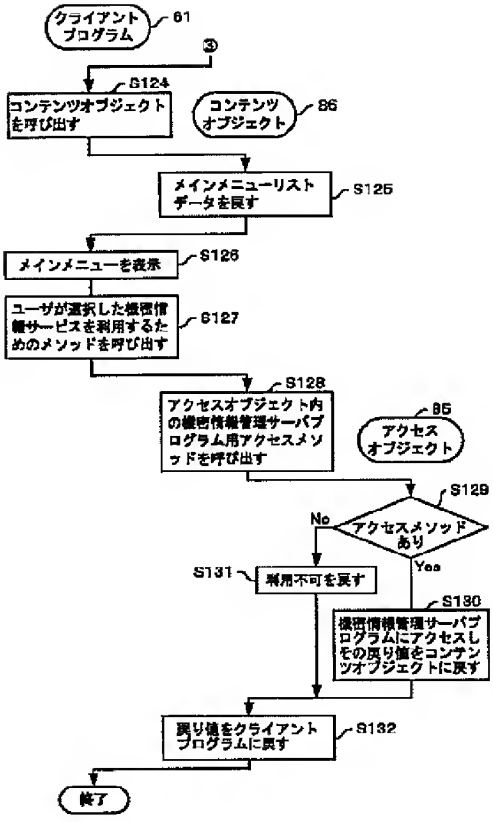
401 アクセスポリシー表

アクセスレベル	機密情報管理サーバプログラム		
	#1	#2	#3
1	1	1	1
2	1	0	1
⋮			

【図５】



【図６】

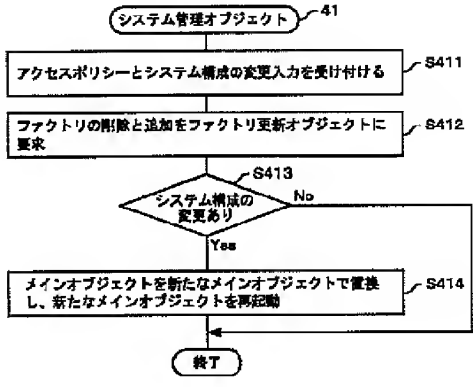


【図１６】

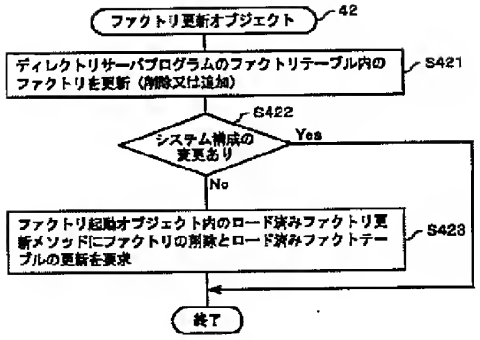
402 システム構成表

機密情報管理サーバプログラム	通信制御情報		
	IPアドレス	ポート番号	通信用デバイスドライバの名称
#1			
#2			
#3			

【図１７】



【図１８】


ファクトリ更新オブジェクト
42
ディレクトリサーバプログラムのファクトリテーブル内のファクトリを更新（削除又は追加）
S421
S422
システム構成の変更あり
Yes
No
ファクトリ起動オブジェクト内のロード済みファクトリ更新メソッドにファクトリの削除とロード済みファクトテーブルの更新を要求
S423
終了